Cassandra Crossing/ Facebook e conto telematico? Ahi ahi, ahi...

(474)—Tutti gli italiani che possiedono account facebook e conto corrente telematico sono in pericolo, e vi spiego perché.

Cassandra Crossing/ Facebook e conto telematico? Ahi ahi, ahi...

(474)—Tutti gli italiani che possiedono account facebook e conto corrente telematico sono in pericolo, e vi spiego perché.

12 aprile 2021—I 24 inarrestabili lettori sanno che Cassandra ama fare sintesi estreme; le sintesi infatti spesso rivelano fatti importanti, assai più di pagine e pagine di informazioni, che al contrario possono nasconderle.

A beneficio di chi non è ancora riuscito a riconoscersi quale vittima di furto di dati personali, e quindi potenziale vittima dello svuotamento del conto corrente, è necessario dire che da poche settimane è certo e dimostrato che praticamente tutti gli utenti facebook italiani (oltre il 90%) hanno i loro dati personali, ed in particolare il numero di cellulare, nei "migliori" database utilizzati dai criminali informatici.

Insisto, praticamente tutti.

Insisto di nuovo, è certo.

Insisto ancora; se il vostro numero non c'era già prima, ora probabilmente c'è ed è "merito" di facebook.

Se volete verificare la cosa, malgrado una strana decisione "censoria" dell'Autorità Garante della Privacy, difesa qui (con poca convinzione) dall'ottimo Guido, **potete usare il servizio gestito da Troy Hunt HaveIBeenPwOwned.**
Inserite il vostro numero di cellulare, completo del prefisso internazionale +39 e senza spazi od altro, e vedrete se il vostro numero di telefono è stato compromesso; se si, scorrendo la pagina dei risultati, vedrete di chi è la colpa.

Veniamo adesso al nocciolo della questione; tutti coloro che, oltre ad un cellulare, hanno anche un conto corrente telematico, e che sfruttano gli SMS come secondo fattore di autenticazione, sono in serio pericolo.

Se invece come secondo fattore, usano l'app della banca, lo sono di meno, ma non di tanto; ci vorrebbe un altro articolo per spiegare il perché, quindi procediamo occupandoci solo di chi usa gli SMS.

Ricevere sul proprio cellulare un SMS per recuperare la password di un account qualsiasi, o per autorizzare l'esecuzione di un bonifico telematico, è un metodo comunissimo.

Molto comune è purtroppo diventato un attacco detto di "*SIM Swap*", usato principalmente per impossessarsi del numero di cellulare della vittima, e così telefonare e ricevere SMS al suo posto.

Tutte le banche ne sono perfettamente a conoscenza; troppo poche hanno emesso avvisi specifici per la propria clientela, come questa.

Non è purtroppo difficile; con un po' di ingegneria sociale è facile, per un criminale informatico, convincere non voi ma l'help desk di certi operatori telefonici "*poco attenti*" di essere il titolare della vostra SIM, e chiedere semplicemente la portabilità del vostro numero telefonico su un'altra SIM dell'operatore.

Non c'è' bisogno che sia il vostro operatore od un operatore famoso; il criminale ne sceglierà uno "vulnerabile" e "voglioso" di nuovi clienti (o con un dipendente corrotto).

Da quel momento in poi il criminale riceverà tutte le telefonate e tutti gli SMS destinati a voi, perché a tutti gli effetti si sarà appropriato del vostro numero telefonico, ed il vostro cellulare si scollegherà in maniera irreversibile dalla rete telefonica.

Dal quel momento in poi il criminale sarà in grado di impossessarsi dei vostri account (di qualsiasi servizio) utilizzando il vostro numero di telefono e gli SMS di verifica.

Ovviamente si tratta di attacchi "mirati", quindi prima della fase di SIM swap il criminale si sarà preparato su di voi, conoscerà i vostri account, il vostro conto corrente, l'indirizzo di casa, un sacco di altri dati personali, soprattutto quelli relativi alla posta elettronica.

Se ha violato il vostro account principale di posta, quello che avete comunicato alla banca, manca solo la "mazzata" finale.

La mazzata finale è appunto il SIM swap, dopodiché lo svuotamento del vostro conto corrente, e l'abuso delle vostre carte di credito, sono a portata di mano del criminale.

Cosa si può fare?

Prima di tutto, tenete pochi soldi sul conto corrente telematico, solo quelli per l'operatività ordinaria, ed utilizzate un secondo conto corrente, rigorosamente senza accesso telematico, dove tenere i vostri soldi ed altri beni. Vi costerà 50 o 100 Euro l'anno, ma sono soldi ben spesi.

Seconda cosa; se potete, attivate una seconda SIM, da tenere insieme alla prima in un cellulare dual-SIM, date questo nuovo numero alla banca, e non lo usate mai, e dico mai, per telefonare o per altri motivi.
Usatelo solo per altre cose riservate ed importanti, come l'account della SPID, della firma digitale e poco altro.
Non telefonate, non lo date agli amici più cari, non scrivetelo da nessuna parte.

Terzo di poi, **entrate immediatamente in modalità "allarme rosso" se vedete che il vostro cellulare si scollega dalla rete GSM senza motivo**, particolarmente in una zona di segnale forte.

Se non riuscite a ricollegarlo subito, nemmeno facendolo ripartire, bloccate immediatamente l'operatività del conto corrente, perché potreste essere stati oggetto di un riuscito attacco di SIM swap.

Se è così, sappiate che lo sta facendo un criminale che ha pianificato attentamente cosa fare, e che, probabilmente in pochi minuti, farà tutto quello di male che è in grado di farvi.

Informatevi prima su come fare a bloccare e sbloccare l'operatività del conto corrente, e tenete a portata di mano il numero di telefono da chiamare e tutti i dati necessari.

Controllate di poterlo fare senza disporre del vostro numero di telefono, e che chi controlla il vostro numero di telefono principale non possa a sua volta sbloccarla.

Ricordate; il vostro avversario è un professionista e voi siete dei dilettanti; prendetevi in anticipo tutti i vantaggi possibili.

E ricordatevi di ringraziare facebook (o LinkedIn) per il rischio aggiuntivo che d'ora in poi correrete.

Anche in questo caso, tuttavia, vale il sempreverde avviso di "V" (in "V for Vendetta"):

"*Di chi è la colpa? Sicuramente ci sono alcuni più responsabili di altri che dovranno rispondere di tutto ciò; ma ancora una volta, a dire la verità, se cercate il colpevole… non c'è che da guardarsi allo specchio.*"

By Marco A. L. Calamari on April 12, 2021.

Canonical link

Exported from Medium on January 2, 2024.